సైబర్ క్రైమ్స్

ఆన్లైన్ మోసాలు తీసుకోవలసిన జాగ్రత్తలు



RAJU K

విషయ సూచిక

ముందు మాట

పూర్వం ఎవరైనా చదువుకున్న వాళ్ళు ప్రయాణం చేస్తుంటే చేతిలో పుస్తకం/న్యూస్ పేపర్ ఉండేది, ఆ రోజుల్లో పుస్తకం హస్త భూషణం అనేవారు, ఈ ఆధునిక కాలంలో మొబైల్ ఫోన్‌ని హస్త భూషణంగా చెప్పుకోవచ్చు.

ఈరోజుల్లో ప్రతి ఒక్కరి చేతిలో మొబైల్ ఫోన్ ఉండటం సర్వసాధారణం, చిన్నపిల్లల గేమ్స్ దగ్గర నుండి పెద్దవయస్సు వారి రోజువారి మందులవరకు అంతా ఆన్లైన్.

ఒక రోజులో మనిషి మనిషితో మాట్లాడటం కంటే మొబైల్ ఫోన్ వాడకమే ఎక్కువ.

చాలామంది రోజువారి దినచర్య మొబైల్ అలారంతోను గుడ్‌మార్నింగ్ మెసేజ్లతోను మొదలవుతుంది.

రోజువారి వ్యాపార వ్యవహారాల్లోనూ కంప్యూటర్, ఇంటర్నెట్ మరియు మొబైల్ ప్రాముఖ్యత చాలా ఎక్కువ.

సాధారణ రోజువారీ కూలి నుండి పెద్దపెద్ద వ్యాపారవేత్తల వరకు ప్రతి ఒక్కరికి మొబైల్, బ్యాంక్ అకౌంట్ లాంటివి అతి సాధారణమైన అవసరాలే కాకపోతే ఇదంతా నాణేనికి ఒక వైపు మాత్రమే.

ఇలాంటి పరిస్థితులలో సైబర్ నేరాలు ఆన్లైన్ మోసాలు ఎక్కువ అయ్యాయి.



నా గురించి



నా పేరు రాజు
ఎలాంటి మొబైల్ సిగ్నల్ కానీ ఇంటర్నెట్ కనెక్షన్ సదుపాయం కానీ సరిగ్గాలేని సాధారణమైన పల్లెటూరు మాది.

డిగ్రీ చదువుకునే రోజుల్లో మా నాన్నగారు కొని ఇచ్చిన కంప్యూటర్‌లో ఉన్న Antivirus ఎందుకు అన్న ప్రశ్న నుంచి మొదలైన నా ఎథికల్ హ్యాకింగ్ ప్రయాణం ఒక (CEH) సర్టిఫైడ్ ఎథికల్ హ్యాకర్ అయ్యేంత వరకు వచ్చింది.

సాధారణ మధ్యతరగతి కుటుంబంలో పెరిగిన నేను, కొన్ని సందర్భాలలో కొంత మంది మొబైల్ ఆపరేటర్స్ ఏ కారణం లేకుండా మొబైల్ బాలన్స్ కట్ చేస్తుంటే బాధగా అనిపించేది, ఎండలో వానలో కష్టపడే కూలీలా దగ్గర నుండి చాల సులువుగా ఏసీలలో కూర్చుని డబ్బులు దండుకుంటున్నారు అని అనిపించేది.

ఇదే ఉదాహరణ రోజువారి కూలి, నెలవారి ఉద్యోగి, ఇలా కష్టపడి పని చేసే ప్రతి ఒక్కరికి వర్తిస్తుంది, మొబైల్ బాలన్స్ కంటే పెద్దది బ్యాంక్ బాలన్స్, ఉదాహరణకి ఒక మధ్యతరగతి వ్యక్తి తన పిల్లల చదువుల కోసమో లేక వేరే ఇతర అవసరాల కోసమో బ్యాంకులో దాచుకున్న డబ్బు పోయింది అనుకుందాం, ఇలాంటి పరిస్థితులలో ఆ వ్యక్తి బాధ వర్ణనాతీతం.

ఇలాంటి సందర్భాలెన్నో, ఇలాంటి ఆలోచనలతో ఉన్న నేను తీసుకున్న నిర్ణయం ఎథికల్ హ్యాకర్ అవ్వాలి అని, సైబర్ క్రైమ్స్ ఆపగల్గడంలో నావంతు కృషి చెయ్యాలి అని.



ఫిషింగ్ (PHISHING)



పేరులో చెప్పిన విధంగానే ఫిషింగ్(FISHING) అంటే తెలుగులో చేపలు పట్టడం, ఇలాంటి పద్ధతినే హ్యాకర్స్ ఉపయోగిస్తారు, దీనిని ఫిషింగ్(PHISHING) అంటారు.

ఈ ఫిషింగ్ ఎటాక్‌లో హ్యాకర్స్ ఫేక్(డూప్లికేట్) వెబ్ పేజెస్, ఫోన్ కాల్స్, మెసేజ్, ఈమెయిల్స్ ద్వారా ఎర వేస్తారు.
ఇందులో చిక్కితే హ్యాకర్స్ బుట్టలో పడినట్టే, ఎలా అయితే చేప ఎరని చూసి జాలరికి దొరికిపోతుందో అలానే.

ఉదాహరణకి వెబ్సైట్ ఫిషింగ్, మీరు ఏదైనా ఆన్లైన్ అకౌంట్‌కి లాగిన్ అవ్వాలి అనుకుంటే అందుకు కావాల్సింది
యూసర్ పేరు మరియు పాస్వర్డ్.

ఈ రెండు వివరాలు ఇచ్చిన తర్వాత లాగిన్ బటన్ మీద క్లిక్ చేస్తాం, కానీ

క్లిక్ చేసిన తర్వాత మీరు ఇచ్చిన వివరాలు ఏమఉతాయో ఎప్పుడైనా ఆలోచించారా! సాధారణంగా లాగిన్ మీద క్లిక్ చేసినపుడు, వెబ్సైటు ఆ వివరాలను డేటాబేస్‌లోని వివరాలను చెక్ చేసుకుంటుంది, ఆ తెర్వాత మన అకౌంట్ ఓపెన్ అఉతుంది, కానీ ఇదే ప్రాసెస్‌లో మీరు ఎంటర్ చేసిన వివరాలు ఒక ఫిషింగ్ పేజీలో నుండి వెళ్తే అవి హ్యాకర్స్ చేతికి వెళ్తాయి, ఒకవేళ మీరు ఇచ్చిన డీటెయిల్స్ మీ ఆన్లైన్ బ్యాంకింగ్‌వి అయి ఉంటె మీ ఖాతాలో డబ్బులు మొత్తం ఖాళీ.

user name

password

LOGIN

Not registered? Create an account

తీసుకోవలసిన జాగ్రత్తలు

★ THINK BEFORE YOU CLICK A LINK

ఏదైనా ఒక లింక్ క్లిక్ చేసే ముందు ఆలోచించండి. ఒకసారి లింక్‌పైన మౌస్ రైట్ క్లిక్ చేసి copy link address ఆప్షన్ సెలెక్ట్ చేసి మీరు కాపీ చేసిన లింక్‌ని notepad లో పేస్ట్ చేసి చూడండి, లింక్ ఏమైనా అనుమానించదగిందా లేదో చెక్ చేస్కోండి.

ఉదాహరణకి

★ మీరు online SBI కి లాగిన్ అవ్వాలి అనుకుంటే దానికి సంబంధించిన ఒరిజినల్ URL - www.onlinesbi.com.

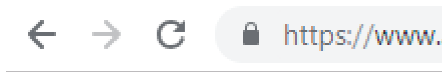
★ www.onlinesb1.com - i ఉండాల్సిన ప్లేస్ లో నెంబర్ 1 ఉంది కాబట్టి ఇది ఒరిజినల్ కాదు.

★ www.0nlinesbi.com - ఇంగ్లీష్ లెటర్ ఓ (O) ఉండాల్సిన ప్లేస్ లో నెంబర్ జీరో (0) ఉంది కాబట్టి ఇది కూడా ఒరిజినల్ కాదు.

★ కొంత మంది హ్యాకర్స్ url shortners ని ఉపయోగించి ఫేక్ లింక్స్ సెండ్ చేస్తారు, అనుమానంగా ఉన్న url యొక్క ఫుల్ url కోసం http://checkshorturl.com/ కి వెళ్లి షార్ట్ url ను పేస్ట్ చేసి చూడండి.

★ ఈ విధంగా హ్యాకర్స్ చాలా రకాలుగా మోసం చెయ్యటానికి ప్రయత్నం చేస్తారు.

★ ఆన్లైన్ బ్యాంకింగ్ సర్వీస్‌లను ఉపయోగించేటప్పుడు url లోని lock సింబల్ ని మరియు https ప్రోటోకాల్‌ని గమనించండి, https ని http ప్రోటోకాల్ తో పోల్చినపుడు డేటా ట్రాన్స్ఫర్ ని సెక్యూర్‌గా ఎన్క్రిప్టెడ్ మోడ్ లో చేస్తుంది, దీని వల్ల హ్యాకర్స్ ఇంటర్నెట్ ద్వారా మనం ట్రాన్స్ఫర్ చేసే డేటాను చూడటానికి అవకాశాలు తక్కువ.



◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇

విషింగ్ (VISHING)





విషింగ్ అంటే ఫోన్ కాల్స్ ద్వారా మాట్లాడి మోసం చెయ్యటం అని అర్ధం (సింపుల్‌గా చెప్పాలి అంటే VOICE +PHISHING).
ఉదాహరణకి మా ఫ్రెండ్‌కి ఒక సంవత్సరం క్రితం ఒక ఒక ఫోన్ కాల్ వచ్చింది అటు వైపు వ్యక్తి మీ నాన్న గారి బ్యాంకు పాలసీ ఒకటి ఉంది మీ బ్యాంకు ఎటిఎం కార్డు వివరాలు చెప్తే ఆ పాలసీ డబ్బులు ఇస్తాం అనటంతో అతను డీటెయిల్స్ చెప్పాడు వెంటనే మొబైల్‌కి ఓటీపీ(వ-న్ టైం పాస్వర్డ్) వచ్చింది, వెంటనే తేరుకున్న మా ఫ్రెండ్ ఓటీపీ డబ్బులు తీసుకోవటానికి కానీ అకౌంట్‌లో డబ్బులు వెయ్యటానికి కాదు కదా! అని అడిగాడు వెంటనే కాల్ చేసిన వ్యక్తి కాల్ కట్ చేసాడు, ఆ తర్వాత ఇదే పద్ధతిని వాడి వాళ్ళ బంధువులు ఓటీపీ చెప్పడం వల్ల 4లక్షలు బ్యాంకు అకౌంట్ నుండి ఖాళీ చేసారు.

ఇలాంటి ఒక సైబర్ క్రైమ్ వల్లనే మా బంధువులలో ఒకరివి 50,000 పోయాయి, తన ఫ్రెండ్‌వి 6లక్షల వరకు

పోయాయి.

ఇలాంటి మోసాల నుండి తప్పించుకోవాలి అంటే ముందుగానే ఇలాంటి మోసాలు ఎలా జరుగుతాయో అవగాహనా వుండాలనేది నా ముఖ్య ఉద్దేశం, ఎందుకంటే చేతులు కాలాక ఆకులు పట్టుకున్నా ఉపయోగం వుండదు కనుక.

తీసుకోవలసిన జాగ్రత్తలు

★ ఏవైనా అనుమానించ దగిన ఫోన్ కాల్స్ వస్తే వ్యతిగత వివరాలు చెప్పక-పోవడం మంచిది .

◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇

స్మిషింగ్ (SMS + PHISHING)

యస్ఎమ్ఎస్(SMS) లను ఉపయోగించి వివరాలను సేకరించి, లేదా మన-ద్వారానే వైరస్‌లను డౌన్లోడ్ చేసుకొనేలా చేసి మోసగించటాన్ని స్మిషింగ్ లేదా SMS PHISHING అంటారు.

ఉదాహరణకి:

- మీరు పదివేలు గెలుచుకున్నారు మీ వివ-రాలను ఇవ్వటానికి ఈ లింక్ క్లిక్ చెయ్యండి అని వచ్చే మెసేజ్ లు.
- మీరు బంగారు/వెండి నాణెం లేదా ముత్యాలు/పెండెంట్లు గెలుచుకున్నారు మీ వివరాలను ఇవ్వటానికి ఈ లింక్ క్లిక్ చెయ్యండి అని వచ్చే మెసేజ్లు లేదా అకౌంట్ కి డబ్బులు పంపండి గిఫ్ట్ పోస్ట్‌లో పంపిస్తాం అని వచ్చే మెసేజ్‌లు, కాల్స్.





- మీరు కార్/బైక్ గెలుచుకున్నారు మీ వివ-రాలను ఇవ్వటానికి ఈ లింక్ క్లిక్ చెయ్యండి అని వచ్చే మెసేజ్‌లు.
- మోడీ గారు ప్రేమతో అందరికి ఫ్రీ రీఛార్జ్ ఇస్తున్నారు నేను కూడా ఆశ్చర్యపోయాను మీరు కూడా రీఛార్జ్ చేసుకోవటానికి ఈ లింక్ క్లిక్ చెయ్యండి అని వచ్చే మెసేజ్‌లు.
- ఈ మెసేజ్‌ని 10 గ్రూప్స్‌లో షేర్ చెయ్యండి 100 రూపాయల టాక్ టైం పొందండి అని వచ్చే మెసేజ్‌లు మొదలైనవి.

తీసుకోవలసిన జాగ్రత్తలు

⋆ మెసేజ్‌ల ద్వారా మీ వ్యక్తిగత వివరాలు నమ్మకం లేని వ్యక్తులకి చెప్పకండి.

⋆ ఏవైనా ఆఫర్స్ అని మెసేజ్‌లు వచ్చినపుడు ముందు అది నిజమో కాదో తెలుసుకొనే ప్రయత్నం చెయ్యండి.

⋆ ఏవైనా లింక్స్ క్లిక్ చేసే ముందు అవి షార్ట్ URL అయితే ఉదాహరణకి tin12e.cc/example.com ని check short url అని నెట్లో సెర్చ్ చేసి ఒరిజినల్ url ని గమనించండి లేదా http://checkshorturl.com/ కి వెళ్లి షార్ట్ urlను పేస్ట్ చేసి చూడండి.

◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇

పాస్వర్డ్స్ (PASSWORDS)



హ్యాకర్స్ పాస్వర్డ్స్ క్రాక్ చేసే పద్ధతుల్లో చాల సులువైన పద్దతి గెస్సింగ్

ఉదాహరణకి :

- 9xxxxxxxxxx - మీ మొబైల్ నెంబర్ ని మీ పాస్వర్డ్గ పెట్టుకోవటం
- RAJU@123 - మీ పేరు చివర @ 123
- R@ju123 - a=@
- password - పాస్వర్డ్ని పాస్వర్డ్గ పెట్టుకోవటం
- P@ssword - a=@
- passw0rd - o=O
- qwerty, asdf - keyboard type learning combinations
- 1234 - Number series
- 123456789 - Number sries
- SIRI@2007 -
- Lucky15$ -
- Chandu@13
- - పాస్వర్డ్ని ఖాళీగా ఉంచటం అంటే ఏ పాస్వర్డ్ లేకుండా లాగిన్అవ్వటం.

తీసుకోవలసిన జాగ్రత్తలు

★ మీ పాస్వర్డ్ స్ట్రాంగ్‌గా వుండాలి అంటే కనీసం 8అక్షరాల పాస్వర్డ్ అయ్యి ఉండాలి.

★ పాస్వర్డ్ (Special Characters) ప్రత్యేకమైన అంకెలు అక్షరాలు వాడటం వలన పాస్వర్డ్ మరింత భద్రంగా ఉంటుంది.
ఉదాహరణకి : ! @ # $ % & ★ మరియు అంకెలు 0-9, ఆల్ఫాబెట్స్ A-Z, a-z అయి వుండాలి ఉదాహరణకి: Mr#!37b2.
ఫోన్ నంబర్స్, పేరుతో ఉండే raju, raju123 లాంటి పాస్వర్డ్స్‌తో పోల్చినపుడు Mr#!37b2. స్ట్రాంగ్ పాస్వర్డ్‌గా చెప్పవచ్చు.

★ ఒకేలాంటి పాస్వర్డ్స్ అన్ని అకౌంట్స్‌కి వాడకూడదు
ఉదాహరణకి : gmail, facebook, mobile, UPI payments(Google Pay, Phone pe కి ఒకేలాంటి పాస్వర్డ్స్ వాడకుండా వేరు వేరు పాస్వర్డ్స్ వాడటం మంచిది .

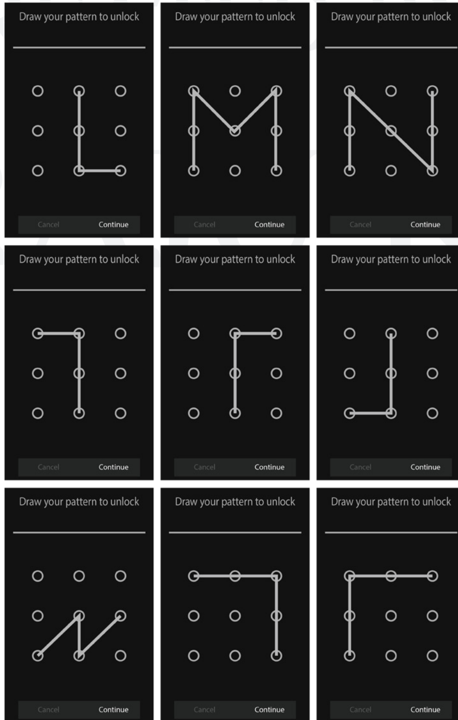
★ పాస్వర్డ్‌గా మీ పేర్లు , మీ పిల్లల పేర్లు , మీ పెంపుడు జంతువుల పేర్లు , మీ కిష్టమైన క్రికెట్, ఫుట్ బాల్ లేదా ఇతర గేమ్స్ టీం పేర్లు మొదలైనవి వాడకండి.



పాస్వర్డ్స్, పాటర్న్స్ (patterns), UPI పేమెంట్స్

ఈ మధ్యకాలంలో యూపీఐ పెమెంట్స్ చాల తక్కువ టైంలో ఎక్కువ పాపులర్ అయ్యాయి (ఉదాహరణకి: Google Pay (TEZ), Phone Pe) ఈ పెమెంట్స్ చెయ్యటం ఎంత సులువో ఎవరికైనా పాస్వర్డ్ తెలిస్తే డబ్బులు పోవటం కూడా అంతే సులువు.

కొన్ని సింపుల్ పాటర్న్స్ (Patterns)



తీసుకోవలసిన జాగ్రత్తలు

★ మొబైల్ లాక్‌కి పాటర్న్ లాక్ పెడితే సింపుల్‌గా ఎవరైనా గెస్ చేసే విధంగ పెట్టకండి.

★ పాటర్న్ లాక్ వాడితే గెస్ చెయ్యటానికి కష్టంగా ఉండే పాటర్న్ వాడండి.

★ ఫోన్ లాక్‌కి UPI పెమెంట్స్ అప్లికేషన్స్‌కి ఒకేలాంటి పాటర్న్ లాక్ కానీ , నంబర్ పాస్వర్డ్ కానీ వాడొద్దు.

★ ఇదే విధంగా whatsapp లాంటి చాటింగ్ అప్లికేషన్స్‌కి ఇతర అప్లికేషన్స్ కి లాక్ వాడుతున్నట్లైతే ఫోన్ లాక్, పాటర్న్ లాక్, నంబర్ లాక్కి ఒకేలాంటి పాస్వర్డ్ వాడొద్దు

◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇

వైరస్



వైరస్ ఒక మాల్వేర్ (Malicious + Software = Malware) ఇందులో రకాలు ఉన్నాయి Virus, Worm, Trojan, Adware మొదలైనవి ఇవన్నీ డేంజరస్ సాఫ్ట్వేర్ అయినప్పటికీ ఒక్కొక్క వైరస్ ఒక్కో రకంగా పని-చేస్తుంది.

ఉదాహరణకి : వైరస్ వల్ల హ్యాక్ ఐన కంప్యూటర్లో ఉన్న సాఫ్ట్వేర్ సరిగ్గా పని చెయ్యదు, ఫైల్స్ డిలీట్ అఉతాయి, కంప్యూటర్ క్రాష్ అవుతుంది.
ట్రోజన్ (Trojan) వల్ల హ్యాకర్ కి ట్రోజన్ ఎటాక్ అయిన కంప్యూటర్ రిమోట్ యాక్సిస్ వెళ్తుంది, దీనితో హ్యాకర్ కంప్యూటర్ ని కంట్రోల్ చెయ్యొచ్చు, ఫైల్స్ అప్లోడ్, డౌన్లోడ్, డిలీట్, కంప్యూటర్ ఆఫ్ చెయ్యొచ్చు, హ్యాక్ అయిన కంప్యూటర్ ని (Botnet)బాట్నెట్ లా ఉపయోగించు కొని వేరే కంప్యూటర్ ని ఎటాక్ చెయ్యొచ్చు.
మీరు ఎప్పుడైనా ఆన్లైన్ షాపింగ్ చేసినపుడు ఆ పేజీ క్లోజ్ చేసి facebook లేదా ఇతర సోషల్ మీడియా సైట్స్ ఓపెన్ చేసినపుడు మీరు ఆన్లైన్ షాపింగ్ లో సెర్చ్ చేసిన వస్తుఉల advertisements చూసే ఉంటారు దీనికి కారణం Adware అనే సాఫ్ట్వేర్.

వైరస్ కంప్యూటర్/మొబైల్‌లో ఎలా ఇన్స్టాల్ అవుతుంది?

ఈమెయిల్స్‌లో వచ్చిన లింక్స్ ఓపెన్ చేసినపుడు.

టెక్స్ట్ మెసేజ్‌లలో వచ్చిన లింక్స్ ఓపెన్ చేసినపుడు.

ఇంటర్నెట్ నుంచి మనకు కావలసిన ఫైల్ పేరుతో వైరస్‌ఫైల్ వుండి వైరస్ ఫైల్ డౌన్లోడ్ చేసుకున్నప్పుడు.

పోర్నోగ్రఫిక్ సైట్స్ ఓపెన్ చేసినపుడు.

ఏవైనా పైరేటెడ్ సాఫ్ట్వేర్/మూవీస్ కోసం ట్రై చేసినపుడు బ్రౌసర్ ఎక్స్టెన్షన్ డౌన్లోడ్ చేసుకున్నప్పుడు.

.apk మరియు .dll ఫైల్స్



చాలా మంది గేమ్స్ లేదా యాప్స్ ఆన్లైన్ డబ్బులు పెట్టి కొనడం ఇష్టం లేక కొన్ని వెబ్సైట్స్ నుండి ఫ్రీగా .apk ఫైల్స్‌ను డౌన్లోడ్ చేసుకొని ప్రైవసీ సెట్టింగ్స్ లో Unknown sources ఆప్షన్ నుండి Allow installation of apps from unknown sources ఆప్షన్‌ని ఆన్ చేసి డౌన్లోడ్ చేసుకున్న .apk ఫైల్స్‌లను ఇన్స్టాల్ చేస్తారు, ఇదే విధంగా కంప్యూటర్‌లో అయితే .dll ఫైల్స్ లను ఇన్స్టాల్ చేస్తారు ఇలా చెయ్యటం వల్ల ఒకవేళ binders అనే పద్ధతిని ఉపయోగించి ఒరిజినల్ ఫైల్‌కి వైరస్/ట్రోజన్/రూట్ కిట్స్/ RAT రిమోట్ ఆక్సస్ లాంటి ఫైల్స్‌లను జోడించి వుంచిన ఫైల్స్ మీరు డౌన్లోడ్ చేసుకున్న .apk లేదా .dll ఫైల్స్‌తో పాటు వైరస్ ఇన్స్టాల్ అయితే ఇక అంతే సంగతులు, ఇది ఎలా ఉంటుంది అంటే మన వేలితో మన కన్నే పొడుచుకున్నట్టు.

తీసుకోవలసిన జాగ్రత్తలు

ముందుగా వైరస్ రాకుండా ఏంచెయ్యాలి ?

⋆ Antivirus+Antimalware+Antitrojan+Antiworm ను ఇన్స్టాల్ చేసుకోవాలి.

⋆ ఇన్స్టాల్ చేసుకున్న Antivirus ను ఎప్పటికప్పుడు అప్డేట్ చేసుకోవాలి.

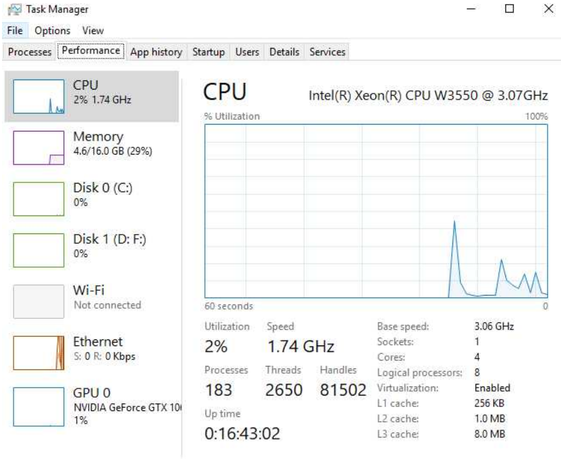
⋆ రెగ్యులర్‌గా మీ కంప్యూటర్/మొబైల్‌లను antivrus తో స్కాన్ చేస్తూ ఉండాలి.

⋆ ఎస్ఎంఎస్(SMS), ఈమెయిల్(EMail), వెబ్సైట్‌లో ఉన్న అనవసరమైన లింక్స్‌కానీ, advertisements కానీ ఓపెన్ చెయ్యకూడదు.

⋆ పైరేటెడ్ సాఫ్ట్వేర్ వాడుతున్నట్లైతే (Educational purpose only not encouraging pirated software) ఇంటర్నెట్ కనెక్టన్ లేని కంప్యూటర్లో వాడటం మంచిది.

⋆ నమ్మకంగా లేని వెబ్సైట్స్ (Untrusted Websites) లింక్స్‌లను ఓపెన్ చెయ్యకూడదు, This web page is not trusted back to safety, Your connection is not private లాంటి బ్రౌసర్ ఎర్రర్ మెసేజెస్‌లను చూసే వుంటారు, సాధారణంగా మనం విసిట్ చేసే వెబ్సైటు http ప్రోటోకాల్ తో ఉండి https(SSL) సర్టిఫికెట్‌లేని వెబ్సైట్స్‌కు ఈ ఎర్రర్ మెసేజ్ వస్తుంది.

⋆ ఫ్రీ ఓపెన్ వైఫై(wifi) లను వాడకండి ఎందుకంటే Rogue access points ల ద్వారా హ్యాకర్స్ మిమ్మల్ని టార్గెట్ చేసే అవకాశాలున్నాయి.



★ మీ కంప్యూటర్/మొబైల్‌కి వైరస్ వచ్చిందని ఎలా తెలుసుకోవాలి ? మీ కంప్యూటర్/మొబైల్ ఫాస్ట్‌గా వర్క్ అయ్యేలా ఎలా చేసుకోవాలి?

★ మీ కంప్యూటర్/మొబైల్ ఇంతకు ముందులా కాకుండా స్లో అవుతున్నా, మీ మొబైల్ డేటా మీరు వాడక పోయిన డేటా ఎక్కువ అయిపోతున్నా, ఏవైనా యాప్స్ ఓపెన్ చేసిన వెంటనే క్రాష్ అవుతున్నా, అనవసరమైన advertisements డిస్ప్లే అవుతున్నా, మీరు ఏ ఆప్స్ వాడకుండా cpu utilization ఎక్కువ ఉన్న మీ మొబైల్/కంప్యూటర్‌కి వైరస్ వచ్చి ఉండవచ్చు.

★ ముందుగా antivirus తో స్కాన్ చెయ్యండి ఏవైనా వైరస్ ఫైల్స్ ఉంటె డిలీట్ చెయ్యండి.

★మీ కంప్యూటర్/మొబైల్లోని కాష్ ఫైల్స్ temporary files లను క్లియర్ చేసుకోండి.

★ ctrl + shift + esc ని ప్రెస్ చేసి Task Manager లోని Processes ట్యాబ్ లో ఏమైనా కంప్యూటర్ కి సంబంధిచినవి కాకుండా వేరే

ఆప్స్ రన్ అఉతూ ఉంటె ఆ process పైన right click చేసి End టాస్క్ ఆప్షన్ పైన క్లిక్ చెయ్యండి.

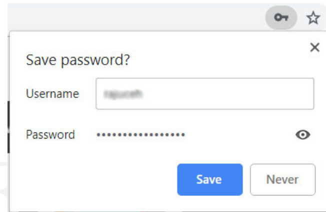
⋆ Performance ట్యాబ్ ఆప్షన్ లో కంప్యూటర్ CPU percenta ge ఎంత యూస్ చేసుకుంటుందో గమనించండి ఒకవేళ percentage utilizatoin మీరు ఏ ఆప్ వాడకుండా ఎక్కువ ఉంటె background లో ఆప్స్ రన్ అఉతున్నాయి అని అర్ధం ఆ ఆప్స్ వైరస్ కి సంబంధిచినవి అయ్యి ఉండవచ్చు.

⋆ అనవసరమైన యాప్స్ కొన్ని కంప్యూటర్ ఆన్ అవ్వగానే auto start అఉతాయి, ఇలా స్టార్ట్ అయ్యే అనవసరమైన ఆప్స్ ని గుర్తించడానికి Startup టాబ్ లోని ఏమైనా అనవసరమైన ఆప్స్ ఉంటె disable చెయ్యండి.

◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇

బ్రౌసర్‌లో పాస్వర్డ్స్ సేవ్ చేస్తున్నారా?

ఇంటర్నెట్ బ్రౌజర్స్‌లో సేవ్ పాస్వర్డ్ అనే ఆప్షన్ ని గమనించే ఉంటారు.



ఇలా బ్రౌసర్లో పాస్వర్డ్స్ సేవ్ చెయ్యటం వల్ల ఎవరైనా వేరే వ్యక్తి మీ కంప్యూటర్ లేదా మొబైల్ బ్రౌసర్ వాడినపుడు వాళ్లకి క్లియర్‌గా ఏ అకౌంట్కి ఏ పాస్వర్డ్ ఉందో క్లియర్‌గా అర్ధం అయిపోతుంది, ఇది ఎలా ఉంటుంది అంటే ఇంటికి తాళం వేసి తాళం చెవి గుమ్మానికి తగిలించి నట్టు.



తీసుకోవలసిన జాగ్రత్తలు

★ మీ బ్రౌసర్‌లోని సెట్టింగ్‌కు వెళ్లి Privacy Security ఆప్షన్ లో save passwords ఆప్షన్‌ని disable చెయ్యండి ఏవైనా passwords ముందుగానే సేవ్ అయ్యిఉంటే డిలీట్ చేస్కోండి.

★ ఇదే విధంగా save address, save creditcard payment details, save auto fill address లాంటివి ఉంటె disble చేసి ఏమైనా saved details ఉంటె క్లియర్ చేసుకోండి.

★ ఇంటర్నెట్ సెంటర్స్‌లో మీ ఆన్లైన్, మెయిల్ అకౌంట్స్‌తో లాగిన్ అవ్వా-ల్సివస్తే జాగ్రత్త వహించండి లాగౌట్ చెయ్యటం మర్చిపోకండి, బ్రౌజర్స్ లో పస్స్వర్డ్స్ సేవ్ చెయ్యకండి.

◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇

ATM (ఎటిఎం)



ఇంతకు ముందు సినిమాలలో లాగ బ్యాంకు రాబరీలు మాస్కు వేసుకొని గన్స్‌తో భయపెట్టి బాగ్లో డబ్బులు తీస్కాని వెళ్లే సీన్స్ ఇప్పుడు లేవు, ఎందుకంటే ఇప్పుడు దొంగలకు కొత్త టెక్నాలజీ అందుబాటులోకి వచ్చింది కాబట్టి సినిమాలలో హ్యాకింగ్ సీన్స్ పెడుతున్నారు.

ఈ మధ్యకాలంలో ATM మరియు బ్యాంక్ నేరాలు చాలా ఎక్కువ అయ్యాయి, ఇలాంటి నేరాలలో చాలా రకాలు ఉన్నాయి అందులో ఒకటి క్లోనింగ్ (cloning).

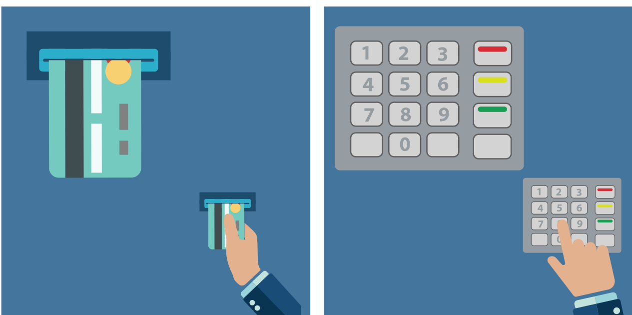
క్లోనింగ్ అంటే సాధారణంగా ఒకేలాంటి వస్తువు వేరొకటి తయారు చెయ్యటం.

ఉదాహరణకి : ఒకేలాంటి మొక్కలు, మనుషులు, జంతువులు.

కార్డు స్కిమ్మింగ్ (క్లోన్) ఎలా అవుతాయి



ఇలా క్రెడిట్ కార్డు, డెబిట్ కార్డులను క్లోన్ చెయ్యటానికి స్కిమ్మర్స్ అనే పరికరాలని వాడుతున్నారు హ్యాక.ర్లు



ఉదాహరణకి: మీరు ఏదైనా హోటల్ కి వెళ్లారు అనుకుందాం, తినడం అయిపోయిన తర్వాత బిల్ కార్డుతో పే చేద్దాం అనుకున్నారు
దీని కోసం హోటల్స్ సాధారణంగా వాడే పద్ధతి బిల్ పైన కార్డు పిన్ నెంబర్ రాసి ఇవ్వటం, ఆ నెంబర్ని తీసుకొని వాళ్ళు హోటల్ లోపలి రూమ్‌కి వెళ్లి అమౌంట్ స్వైప్ చేసి బిల్ తెచ్చి ఇస్తారు.
ఈ పద్ధతి వల్ల స్వైపింగ్ మెషిన్‌కి బదులు స్కిమ్మర్స్ వాడి మీ కార్డు డీటెయిల్స్ మొత్తం క్లోన్ చెయ్యొచ్చు, కార్డు క్లోన్ అయ్యాక ఆ డీటెయిల్స్ డూప్లికేట్ కార్డుతో మీరు ముందుగా రాసి ఇచ్చిన పిన్ నెంబర్ వాడి మీ అకౌంట్లో డబ్బులు డ్రా చేస్తారు.

ఈ స్కిమ్మర్స్ ఉపయోగించి ఏటిఎం లలో డూప్లికేట్ కీప్యాడ్ , డూప్లికేట్ స్వైపింగ్ పరికరాలను పెట్టి ఉంచుతారు, ఇలాంటి స్కిమ్మర్స్ లో ఎవరైనా స్వైప్ చేసిన తర్వాత హ్యాకర్స్ తమ కంప్యూటర్లలోకి కార్డు డేటాను సేవ్ చేసుకొని అలానే ఉండే మరొక డూప్లికేట్ కార్డును తయారు చేస్తారు, డూప్లికేట్ కీప్యాడ్ నుండి సంపాదించిన పిన్ నెంబర్‌ను వాడి మీ అకౌంట్ లో ఉన్న డబ్బును తీసుకుంటారు.

ఇదే విధంగా కొంతమంది ఎటిఎంలో మీ వెనకాల నిల్చుని మీ పాస్వర్డ్ ని చూసే ప్రయత్నం చేస్తారు.

తీసుకోవలసిన జాగ్రత్తలు

★ ATM లో లేదా, షాపింగ్ మాల్స్‌లో మీఅకౌంట్ పిన్ ఎంటర్ చేసేటప్పుడు మీరు ఎంటర్ చేసే పిన్ కనబడకుండా చెయ్యి అడ్డు పెట్టి పిన్ ఎంటర్ చెయ్యటం అలవాటు చేసుకోండి.

★ స్వైపింగ్ మెషిన్లో కార్డ్ చిప్ వరకు లోపలి వెళ్లిందా అంతకంటే ఎక్కువ లోపలి స్వైప్ అవుతుందా గమనించండి ఒకవేళ ఎక్కువగా తేడా అనిపిస్తే జాగ్రత్తవహించండి.


QUITTUNG
KARTE




CASH


AIB
BANKLINK

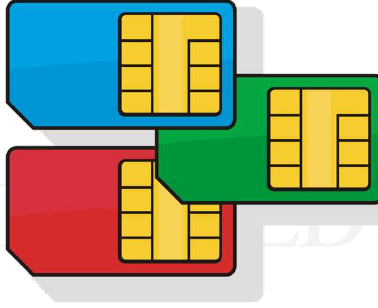
★ ATM లో కార్డు స్వైప్ చేసే ముందు ఒకసారి ఆ స్వైప్ చేసే మెషిన్ ఏరియా ని, పిన్ ఎంటర్ చేసే కీప్యాడ్‌ని కొద్దిగా లాగి చూడండి, ఒకవేళ ఏమైనా డూప్లికేట్ స్కిమ్మర్స్ కానీ , కీపాడ్స్ కానీ ఉన్నాయేమో గమనించం-డి, మీ కార్డు డీటెయిల్స్ కరెక్ట్‌గా ఉండి కూడా మీ కార్డు ఎర్రర్ వస్తున్న, గ్రీన్ లైట్ ఆగకపోయిన లేదా అలాగే వెలుగుతూ ఉన్న జాగ్రత్తపడండి.

★ ఏమి లేకపోయినా ఉడుత హడావిడి చేసినట్టు ATM దగ్గర షాపింగ్ మాల్స్ లో హడావిడి చెయ్యకుండా పైనచెప్పిన విషయాలని జాగ్రత్తగా గమ-నించండి.

★ ఏమైనా నకిలీ పరికరాలు ATM లలో కనిపిస్తే వెంటనే 100 కి కాల్ చేసి పోలీస్‌లకు చెప్పండి.

◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇

సిమ్ కార్డు స్వాపింగ్



సిమ్ స్వాపింగ్ ద్వారా మన సిం కార్డు లాంటి సిం మరొకటి తయారు చేస్తారు.
ఇలా చేసిన సిం కి మన మొబైల్ నెంబర్ ఆక్టివేట్ అవుతుంది, తర్వాత మన బ్యాంకు నుండి వచ్చే OTP(ఓటీపీ) స్వాప్ అయిన సిం కి వెళ్తుంది.

OTP ఉంటె ఖాతాలో డబ్బులు ఖాళి
అందుకే బ్యాంకు నుంచి వచ్చే ఓటీపీ తో పాటు ఓటీపీని ఎవరితో షేర్ చెయ్యొద్దు అని చెప్తారు.

సిమ్ స్వాపింగ్ ఎలా చేస్తారు ?

సిమ్ కార్డు వెనుక ఉండే ౨౦ అంకెల నెంబర్ చాలా ముఖ్యమైనది
ఈ పద్ధతి సిం కార్డు పోర్ట్ చెయ్యటం లాంటిది.
మీ నెట్వర్క్ సరిగ్గా లేదని, కొత్త సెట్టింగ్స్ చేసుకోవాలి అని, లేదా మీ పాత

సిమ్‌ని కొత్త సిమ్‌తో మారిస్తే కానీ మీ మొబైల్ నెంబర్ పని చెయ్యదు అని, లేదా మీ 3జి మొబైల్‌ను 4జి/5జి మార్చు కోవాలి అని ఇంకా రకరకాల కారాణాలను చెప్పి మీ సిం వెనుక 20 అంకెల నెంబర్ చెప్పమంటారు తర్వాత ఈ 20 అంకెల నెంబర్‌ని ఉపయోగించి ముందుగానే సేకరించిన మీ ఆధార్ కార్డు లేదా ఇతర వ్యతిగత వివరాల ద్వారా టెలిఫోన్ ఆపరేటర్ నుండి కొత్త సిం తీసుకుంటారు.

తీసుకోవలసిన జాగ్రత్తలు

★ ఏవైనా అనుమానించ దగిన ఫోన్ కాల్స్ వస్తే వ్యతిగత వివరాలు చెప్పక-పోవడం మంచిది.

◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇

పైరేటెడ్ సాఫ్ట్వేర్

సాధారణంగా ఏదైనా సాఫ్ట్వేర్ కొనాలి అంటే దాని విలువను బట్టి వేళ రూపాయల నుండి లక్షల్లో ఉంటుంది.

ఇలాంటి సాఫ్ట్వేర్‌ల కోసం చాల మంది పైరేటెడ్ సాఫ్ట్వేర్‌ని ఉపయోగించి CRACKS కంప్యూటర్లో ఇన్స్టాల్ చేస్తారు.

ఇలా ఇన్స్టాల్ చేసిన క్రాక్స్ తో పాటు వైరస్ మరియు హ్యాకర్స్ ఉపయోగించే బ్యాక్ డోర్స్ ఇన్స్టాల్ అవ్వటం చాలా ఎక్కువ.

తీసుకోవలసిన జాగ్రత్తలు

★ పైరేటెడ్ సాఫ్ట్వేర్ వాడుతున్నట్లైతే (Educational purpose only not encouraging pirated software) ఇంటర్నెట్ కనెక్టన్ లేని కంప్యూటర్లో వాడటం మంచిది



పబ్లిక్ ప్లేసెస్‌లో ఫ్రీ వైఫై (FREE WIFI) వాడుతున్నారా?



FREE
Wi Fi

ఈ రోజుల్లో బస్ స్టాప్స్, షాపింగ్‌మాల్స్, హోటల్స్‌లో కస్టమర్స్‌ని అట్రాక్ట్ చెయ్యటం కోసం ఫ్రీగ వైఫై ఇస్తున్నారు.

ఇలా ఫ్రీగ వైఫై వాడినపుడు ఎవరైనా హ్యాకర్ కంట్రోల్లో ఉన్న వైఫై కి కనెక్ట్ అయితే మీరు వాడే డేటాను డిక్రిప్ట్ చేసి పాస్వర్డ్స్, యూసర్ నేమ్స్, కార్డు డీటెయిల్స్ మొదలైన వివరాలను వాడి బ్యాంక్ అకౌంట్లో డబ్బులు దొంగిలించే ప్రయత్నం చేస్తారు.

తీసుకోవలసిన జాగ్రత్తలు

★ ఫ్రీ వైఫై వాడేటప్పుడు బ్యాంకు సంబంధించిన లావా దేవీలు చెయ్యకపోవడం మంచిది.
అతి ముఖ్యమైన డేటా ట్రాన్స్ఫర్ జరిగే వాడకం తగ్గిస్తే మంచిది.



జ్యూస్ జాకింగ్

మొబైల్ ఫ్రీ ఛార్జింగ్ చేసుకుంటున్నారా! జ్యూస్ జాకింగ్ గురించి తెలుసుకోండి

జ్యూస్ జాకింగ్ పద్దతితో ఛార్జింగ్ పోర్ట్స్ నుండి మన డేటాని జ్యూస్ లా పిండేస్తారు




తీసుకోవలసిన జాగ్రత్తలు

★ ప్రయాణ సమయాలలో పవర్ బ్యాంకు లను వాడటం
USB charging only ఆప్షన్ ను enable చెయ్యటం
మీ సొంత చార్జర్‌లను అడాప్టర్‌తో సహా వాడటం

సోషల్ మీడియాలో మనం దొంగలకు, హ్యాకర్స్‌కి ఏం చెప్తున్నాం?

సోషల్ మీడియాలో కొంత మంది షేర్ చేసే వివరాలు ఇలా ఉంటాయి

- In a relationship oct-3-2018
- Got engaged Jan-1-2019
- Got married feb-13-2019
- First Baby Nov-5-2019
- 2nd Baby Aug-15-2020
- My Baby Name Sana
- My Baby Nick name PINKY
- My new pet name Snoopy
- My new mobile number 9xxxxxxxxx

ఇలా పర్సనల్ డీటెయిల్స్ షేర్ చేసుకోవటం వల్ల హ్యాకర్స్ మీ డీటెయిల్స్‌ని మిస్ యూస్ చేస్తారు.

లేదా family trip to Tirupathi tomorrow, Going out for birthday celebrations లాంటి పోస్ట్లు చూసినపుడు ఎవరైనా దొంగలు మీ ఇంట్లో దొంగతనం ప్లాన్ చేసుకుంటారు.

లేదా My Baby like pink color Ice cream అని పెట్టి మూతి ముందుకి పెట్టి రెండు వేళ్ళు చూపించి మీ పిల్లలతో సెల్ఫీ అప్లోడ్ చేసారు అనుకుందాం, తరువాతి రోజు ఎవరైనా కిడ్నాప్ చేసే ప్లాన్స్ ఉంటె అదే పింక్ కలర్ ఐస్క్రీం ఇచ్చి కిడ్నాప్ చేసే అవకాశాలు ఉన్నాయి.

తీసుకోవలసిన జాగ్రత్తలు

★ THINK BEFORE YOU SHARE

★ఏమైనా సోషల్ మీడియాలో షేర్ చేసే ముందు ఆలోచించండి.

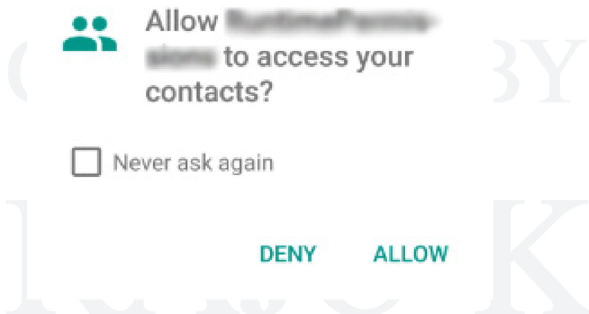


★ఈ మధ్యకాలంలో ఫొటోస్‌లో ఉన్న ఫింగర్స్ ఆధారంగా డూప్లికేట్ ఫింగర్ ప్రింట్స్ తయారుచేసే టెక్నాలజీ వచ్చింది.



మన పర్సనల్ డీటెయిల్స్ ఫైల్స్ (Internet)నెట్లోకి ఎలా వెళ్తున్నాయి?

మనం ఏవైనా ఆప్స్ ఇన్స్టాల్ చేసుకునేటప్పుడు apps permissions అడ-గటాన్ని గమనించే ఉంటారు - Images, Camera, Microphone, call permissions, మొదలైనవి.



True Caller లాంటి ఆప్స్ వాడటం వల్ల మన contact నెంబర్ తో పాటు ఇతరుల కాంటాక్ట్ నంబర్స్ ని కూడా షేర్ చేస్తున్నాం, ఇలా ఇతరులను కూడా ఇబ్బంది పెడుతున్నాం.

Google సెర్చ్ ఇంజిన్, మ్యాప్స్ ఇంకా ఇతర ఫీచర్స్ మనకి ఎంతగా ఉపయోగ పడుతున్నాయి అంతే పర్సనల్ డీటెయిల్స్ ని సర్వర్స్ లో సేవ్ చే-స్తున్నాయి, ఒకసారి Google My Activity కి వెళ్లి చూడండి, మీరు మర్చి పోయిన వివరాలు కూడా పలానా తారీఖున మీరు ఎ ప్రయాణం చేసారు ఏ వెహికల్ మీద ఎంత సేపు జర్నీ చేసారు, ఏం ఫోటోస్ తీశారు , ఇంటర్నెట్ లో ఏం సెర్చ్ చేశారు ప్రతి విషయం సేవ్ అయ్యి ఉంటుంది.

My Activity

Search

Filter by date & product

Only you can see this data. Google protects your privacy and security. Learn

Today

Some activity may not appear yet

ITEMS 61 | ANDROID | VOICE & AUDIO | ASSISTANT | SEARCH | ADS

Item view

Selection

Delete activity by

Other Google activity

Activity controls

Help

Send feedback

తీసుకోవలసిన జాగ్రత్తలు

★ అనవసరమైన ఆప్స్ డౌన్లోడ్ చేసుకొని వాటికి మన పర్సనల్ డేటా accessని ఇవ్వకండి, అవసరం లేని ఆప్స్ ని వెంటనే uninstall చేస్కోండి.

★ activity అనవసరం అనుకుంటే డిలీట్ చేస్కోండి, అవసరం లేని activities ని diable చేస్కోండి.

★ వినటానికి కష్టంగా ఉన్న, పాతరకం నెట్ కనెక్షన్ లేని బ్లాక్ అండ్ వైట్ ఫోన్ లు ఇప్పటి స్మార్ట్ మొబైల్స్ కంటే సెక్యూరిటీ ఎక్కువ, ఇలాంటి పాత మొబైల్స్ పైన ఎటాక్ జరిగితే అది కేవలం స్మిషింగ్, విషింగ్ లాంటి అతి తక్కువ అటాక్స్ మాత్రమే జరుగుతాయి.

◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇

సోషల్ మీడియా అకౌంట్స్ హ్యాక్ అయితే ప్రమాదమా?

ఈ రకమైన సైబర్ క్రైమ్‌ని (Identity theft)ఐడెంటిటీ తెఫ్ట్ గా చెప్పవచ్చు, మీ పేరు డీటెయిల్స్‌ని ఉపయోగించి ఫేక్ ప్రొఫైల్‌ని సృష్టించడం, ఫేక్ డాకుమెంట్స్ చెయ్యటం, మీ బంధువులు స్నేహితుల దగ్గరనుండి అర్జెంటు గా డబ్బులు కావాలి అని మెసేజ్ పంపి హ్యాకర్స్ బ్యాంక్ అకౌంట్ నంబర్స్ ఇస్తారు.

వేరే వ్యక్తులను బయపెట్టటం, మోసం చెయ్యటం, అసభ్యమైన మెసేజ్ లను పంపించడం జరిగే ప్రమాదం ఉంది

తీసుకోవలసిన జాగ్రత్తలు

★ రెగ్యులర్ గా పాస్వర్డ్స్‌ని చేంజ్ చేస్తూ ఉండండి



మనం రిజిస్టర్ కాకుండా మన మొబైల్ నెంబర్‌కి ఆఫర్స్ మెసేజ్లు ఎలా వస్తున్నాయి?

షాపింగ్ మాల్స్‌కి వెళ్లినపుడు కొంతమంది ఆఫర్స్ ఉన్నాయ్ డీటెయిల్స్ ఫిల్ చెయ్యండి అని అని కార్డ్స్ ఇస్తారు, వీళ్ళు కాలేచ్ట్ చేసిన డేటా కొంతమంది టెలి మార్కెటింగ్ వాళ్ళు కొంటారు, ఇలా చేతులు మారిన మొబైల్ నంబర్స్ మరియు డేటా చివరికి హ్యాకర్స్ చేతిలోకి వెళ్తే చాలా ప్రమాదం.

షాపింగ్ చేసినపుడు బిల్లింగ్ కౌంటర్ దగ్గర మనం ఇచ్చే నంబర్స్‌కి ఆఫర్స్ మెసేజ్లు వస్తాయి.

True Caller లాంటి ఆప్స్ కి manage contacts అండ్ phone calls ఆప్షన్‌ని enable చేసినపుడు.

తీసుకోవలసిన జాగ్రత్తలు

★ ఆఫర్స్ అనగానే నిజమో కాదో తెలుసుకోకుండా ఆత్రంగా డీటెయిల్స్ ఇవ్వకండి.



Fake News(పుకార్లు)

పెద్దలు ఒక మాట అంటారు పుకార్లు బాగా షికార్లు చేస్తాయి అని, అయితే ఈ పుకార్లు (fake news) ఇంటర్నెట్ లేని కాలంలో మనం ఉండే పరిసరాలు, ఊరు వరకే పరిమితంగా ఉండేవి కానీ ఇప్పుడు దేశాలు దాటిపోతున్నాయి

ఇలాంటి ఫేక్ న్యూస్‌ల వల్ల ఎవరైనా నిజంగా అత్యవసర న్యూస్ ఏదైనా చెప్పినా నమ్మకం కలగదు

ఫేక్ న్యూస్ ఎలా ఉంటాయి ?

హిమాలయాల్లో అద్భుత పుష్పం వికసించింది, మీరు కూడా దర్శించుకుని పరవసించండి

ఈ మెసేజ్ ఓపెన్ చేసి మీ మొబైల్ ఫుల్ ఛార్జింగ్ చేసుకోండి ఏ మెసేజ్ ని ఒక యూనివర్సిటీ ప్రొఫెసర్ తయారు చేసారు చూసి నేను కూడా ఆశ్చర్యపోయాను అని

ఈ ఫొటోలోని అమ్మాయికి కళ్ళు లేవు ఈ మెసేజ్ ని షేర్ చెయ్యటం ద్వారా whatsapp/facebook వాళ్ళు షేర్ కి ఒకరూపాయి డొనేట్ చేస్తారు అని

ఆడవాళ్ల సేఫ్టీ కోసం క్యాబ్స్ లో ప్రయాణం చేసేటప్పుడు ఈ నెంబర్ కి మీ క్యాబ్ నెంబర్ లొకేషన్‌ని షేర్ చేస్తే పోలీస్ మిమల్ని ట్రాక్ చేస్తారు అని (ఐడియా మంచిదే అయినా ఇందులో నిజం మాత్రం తక్కువ) - ఒకవేళ క్యాబ్ జర్నీ చేసేటప్పుడు ట్రాక్ కావలి అనుకుంటే మన జర్నీ డీటెయిల్స్ షేర్ చేసుకొనే ఆప్షన్ OLA, UBER ఆప్స్‌లో ఉంది)

- మెసేజ్ 10 గ్రూప్స్ లో షేర్ చెయ్యటం ద్వారా డబ్బులు/రీచార్జ్ గెలుచుకోండి అని

పలానా అప్లికేషన్ మన భారతీయులు తయారు చేశారు డౌన్లోడ్ చేసుకొని ఎంకరేజ్ చెయ్యండి అని

ఈరోజు మన ప్రధాని మోడీ గారు Made India నినాదాన్ని గురించి మాట్లాడుతూ WhatsApp అనేది అమెరికా తయారీ అన్నారు. మనకు మనదేశంలో తయారైన Telegram అనే App ఉంది. WhatsAppను చైనా తిరస్కరించింది. చైనీయులు వారి దేశం లో తయారు చేసిన We Chat అనే App ఉపయోగిస్తారు. మరి మన స్వదేశీ App ను ఎప్పుడు ఉపయోగిస్తాం WhatsApp ను ఒకరు ఒక సంవత్సరం పాటు వాడితే అమెరికాకు 56 రూపాయలు చేరుతుంది. ఆలెక్కన 20 కోట్ల మంది ఉపయోగిస్తే మన సొమ్ము 1120 కోట్లు మనకు దక్కకుండా అమెరికాకు చేరుతుంది. కనుక ఈవిషయం అందరికీ తెలిపి స్వదేశీ వస్తువులు అందరూ వాడే విధంగా అవగాహన కలిగించండి ఈసందేశం అందరికీ పంపి Telegram download చేసుకోమని చెప్పండి. WhatsApp కంటే Telegram లో అనేక అదనపు సౌకర్యాలు ఉన్నాయి. Telegram ద్వారా 50mb వీడియోలు పంపవచ్చు. Wordfiles, Excell files, Adobe files గూడ పంపవచ్చు. ఒక గ్రూప్ లో 200మందిని చేర్చవచ్చు. అంతా ఉచితమే. ఇంకా చాలా ముఖ్యమైన విషయం ఏమిటంటే WhatsApp లాగే పనిచేస్తుంది. Interface గూడ WhatsApp నే పోలిఉంటుంది. కనుక ఈ రోజు నుండి మనమందరం Telegram ను ఉపయోగిద్దాం. ఈ సందేశాన్ని మీరు గనుక మీతో contact లో ఉన్న 25 మందికి గనుక పంపిస్తే మీరు 497.54 రూపాయలు విలువ గల ఉచిత talktime పొందుతారు. పంపిన 10 నిమిషాల తర్వాత చెక్ చేసి చూడండి.

FAKE NEWS

Only this Saturday we give our members 1 free spin for a chance to win exclusive prizes!

SPIN

Extra Spin

Only one game allowed per IP.

Like Comment Share Delete

FAKE NEWS

FAKE NEWS

19:43

Plz.forward.PLz don't delete without reading, a girl 18 years"mounika "ECE"STUDENT 3rd year studying in NPTC college.she is in critical stage. She got blood clot In brain.Her frnds need 30 lakhs for operation. All networks agreed to pay10 paise for each msg share please forward atleast 10 members.

chesina cheyyakapoina meeku vachedi ledu.. poyyedi ledu..

This msg was created by
a scientist of DRDO,Hyderabad

Send this msg to 3 groups then check your battery
100% fully charged

NAME:
Contact number: +91

Im also shocked...!!!

It worked...

9:45 PM

FAKE NEWS

🚫DELETE WHATSAPP🚫
Today our PM Modi ji spoke a slogan of Made In India.
Come lets start with using TELEGRAM an Indian app instead of using the American app WhatsApp.
🔹 It is the first Indian social media app.

Think about it...Even the Chinese have refused WhatsApp and adopted the Made in China "WeChat", when we are going to start??
Use Whatsapp for one year & stop it!

Its one year cost is 56 Rupees, and In India there are 20crore Indians....
If we use WhatsApp then 20crore × 56rupees=1120crore rupees will go outside India, to create awareness please send this msg to everyone & download TELEGRAM.

🔘TELEGRAM has more functions then WhatsApp:-
🔸 It can send 50MB video
🔸 It can even send Word, Excel & Adobe files
🔸 In a group, 200 people can be added
🔸 It is free of cost, no charges at all
🔸 The most important thing, it works same as WhatsApp & the interface is also like Whatsapp only..
So today onwards use ❤ TELEGRAM ❤
🇮🇳Indian🇮🇳

Forward this message to 25 WhatsApp contacts. u wil get Rs.497.54 talktime.

Watch in today Times of India newspaper. Page no 7. thank you.

Check your balance after 10min

FAKE NEWS

FAKE NEWS

హిమాలయ పర్వతం
పై "నాగపుష్పం" విరిసింది
ఈ పుష్పము 36 సంవత్సరాల
ఒకసారి విచ్చుకుంటుంది,
చూసేందుకు శేషా నాగ పడగము
వలే ఉంటది. ఈ చిత్రాన్ని
అందరికి షేర్ చేయండి
అందరూ దర్శించుకుంటారు.

తీసుకోవలసిన జాగ్రత్తలు

★ ఏవైనా ఫేక్ న్యూస్ వస్తే వెంటనే షేర్ చెయ్యకుండా నిజమో కాదో తెలుసుకొనే ప్రయత్నం చెయ్యండి, ఒకసారి నెట్లో ఆ న్యూస్ గురించి సెర్చ్ చేసి చూడండి



మీ మొబైల్ పోతే/ఎవరైనా దొంగిలిస్తే ఏం చెయ్యాలి?

★ ముందుగా మొబైల్ కొన్న వెంటనే మొబైల్ బాక్స్, బిల్, జాగ్రత్తగా ఉంచుకోండి.

IMEI నెంబర్ చాలా ముఖ్యమైనది

మీ మొబైల్‌లో ప్లే స్టోర్ కి వెళ్లి Find My Device ఆప్‌ని డౌన్లోడ్ చేసోకండి, తర్వాత మీ ఇమెయిల్ తో లాగిన్ అయ్యి మీ డివైస్‌ని ఆడ్ చేసోకండి, ఈ ఆప్‌ని కంప్యూటర్ లో కూడా బ్రౌసర్ నుంచి ఓపెన్ చేసి ఆపరేట్ చెయ్యొచ్చు.

★ ఒకవేళ Find My Device లాంటి ఆప్స్ ద్వారా మీ మొబైల్ దొరకదు అనుకుంటే మీ డాటాను ఈ ఆప్ ద్వారా erase/డిలీట్ చెయ్యటానికి ట్రై చెయ్యండి, తర్వాత పోలీస్ స్టేషన్‌కి వెళ్లి మీ పోయిన మొబైల్ నెంబర్ IMEI నెంబర్ ఇచ్చి కేసు పెట్టండి, ఇలా చేసిన తర్వాత పోలీస్ డిపార్ట్మెంట్ వాళ్ళు మొబైల్ నెట్వర్క్ ఆపరేటర్స్‌కి మీ IMEI, మొబైల్ నెంబర్ ఇస్తారు, ఇలా ఇచ్చిన నంబర్స్‌ని సెల్యూలర్ టవర్స్ ఆపరేటర్స్ మీరు ఇచ్చిన నంబర్స్ ఆక్టివేట్ అయితే సెల్ టవర్ ఏరియాని బట్టి మీ మొబైల్ ఎక్కడ ఉందో తెలుసుకొనే ప్రయత్నం చేస్తారు.

◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇

★ Facebook–Cambridge Analytica data scandal - United state పొలిటిక్స్‌పై ప్రభావం చూపించినపుడు, ప్రతి రోజు మనం వాడే ఇంటర్నెట్, సెర్చ్ ఇంజిన్స్, ఆప్స్ మన డైలీ లైఫ్ పైన ప్రభావం చూపిస్తున్నాయి అనటంలో సందేహం లేదు.

★ క్రైమ్స్ రోజు రోజుకి రూపుమారుతున్నా జరగడం మాత్రం మానడం లేదు రాబోయే రోజుల్లో సైబర్ క్రైమ్స్ పెరిగే అవకాశాలు చాలా ఎక్కువగా ఉన్నాయి.

★ ముందుగా అవగాహన ఉండటం వల్ల నేరాలను కొంతమేర అదుపులో ఉంచగలుగుతాం.

★ ఒక్కసారి నష్టపోతే ఆ నష్టాన్ని భర్తీ చెయ్యటానికి నెలలు సంవత్సరాలు పట్టొచ్చు లేదా అవ్వకపోవచ్చు.

★ మనిషి ఆలోచన విధానం మారి మంచి మార్గం లో కష్టపడి వచ్చిన ఫలితంతో ఆనందించడం అలవర్చుకోవాలి, వ్యక్తి మారితే వ్యవస్థ మారుతుంది.

★ తెలుగులో మొట్ట మొదటి ఎథికల్ హ్యాకింగ్ & సైబర్ క్రైమ్స్ సంబంధించిన పుస్తకం బహుశా ఇదే ఐవుంటుంది.

SPECIAL THANKS TO MY PARENTS

ఎండలో వానలో కష్టపడి వ్యవసాయం చేసి వాళ్ళు ఉన్న స్థితిలోనే నన్ను చదివించి ఎంతో కొంత మంచి స్థాయిలో ఉంచిన

నా తల్లిదండ్రులకి నా హృదయపూర్వక ధన్యవాదాలు

★★★★★



ఈ పుస్తకాన్ని చదవటానికి మీ విలువైన సమయాన్ని కేటాయించినందుకు ధన్యవాదాలు.

జైహింద్ !

rajuceh@gmail.com